Privacy Preserving HIPAA-Compliant Access Control Model for Web Services

Tariq Alshugran, Advisor: Dr Julius Dichter
Department of Electrical and Computer Engineering,
University of Bridgeport, CT.

Abstract

Most of the modern health-related information is collected, maintained, and accessed through computerized systems. However, the interaction with this information needs to comply with the US federal regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Due to the complexity of healthcare regulations, it's not easy to deploy a complaint system, especially for heterogeneous systems designed to allow data transfer and communication. Web services can be used to solve the problem of incompatible systems intercommunication; however, a generic model for HIPAA enforcement is required. In this paper we propose a generic HIPAA complaint privacy access control model for web services that can be easily applied to any existing covered entity web services.

Purpose of the Study

- Evaluate the requirements and the components that should be available in a privacy preserving HIPAA-compliant access control model for web services.
- Specify the criteria for formalizing HIPAA.
- Find the features required in an access control language to express the formalized rules.
- Create a web service model prototype and that implements the access control model.

HIPAA Overview

- Health Insurance Portability and Accountability Act (HIPAA). Also know as Public Law 104-191.
- Passed by the U.S. Congress on August 1996.
- Privacy laws are specified in Title 2. Preventing health care fraud and abuse (administrative simplification), which includes: transactions and code sets; identifiers; privacy; and security. The concentration of this work will be on the privacy section of the law, more specifically, section 164.
- Very complex and dense, hard to use as a guide by software developers.

HIPAA Formalization Criteria

Any formalization should be:

- Complete and cover all the privacy rules in HIPAA .
- Context-based: Extract any law context including the roles, purposes, etc.
- Exception handling: handle the rule itself and any exception to the rule

Access Control language

Apply the formalized rules to form an access control that can handle any request formatted as:

ALLOW [Data User]
TO PERFORM [Operation] ON [Data Type]
FOR [Purpose] PROVIDED [Condition]
CARRY OUT [Obligation]

Web Services

- Software system designed to support interoperable application-to-application interaction over a network.
- Web services utilize a set of eXtensible Markup Language (XML)

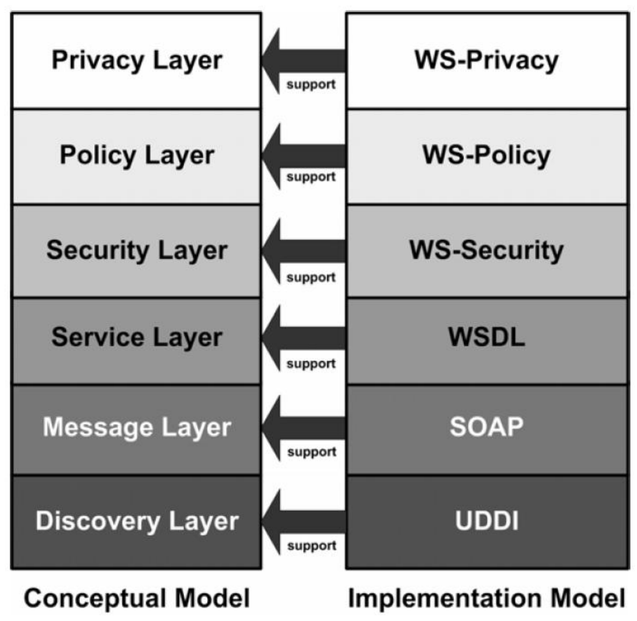
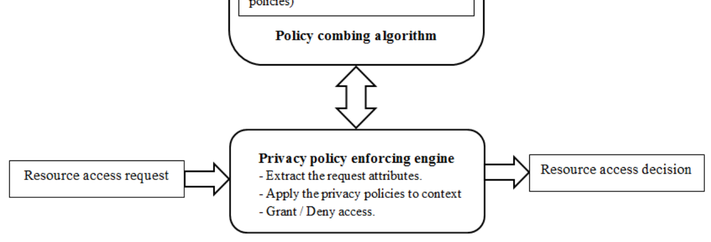


Fig. 1. Web service conceptual and implementation models mapping

Model Prototype



Conclusion and Future Work

- Create a prototype of the proposed privacy access control model.
- Pointed out the model components and each component requirements.
- Still need to carry out an extensive detailed research for each component.
- Put all the pieces together to implement the proposed model.

References

[1] S. J. Dwyer III, A. C. Weaver, and K. K. Hughes, "Health Insurance Portability and Accountability Act," *Security Issues In The Digital Medical Enterprise*, vol. 72, no. 2, pp. 9–18, 2004.
[2] W3S, "Web Services Glossary," 2004. [Online]. Available: http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/#webservice. [Accessed: 21-May-2013].
[3] J. K. Zhang and W. Xu, "Web Service-based Healthcare Information System (WSHIS): A Case Study for System Interoperability Concern in Healthcare Field," in *International Conference on Biomedical and Pharmaceutical Engineering*, 2006, pp. 588–594.
[4] S. Chattejee, "Developing Enterprise Web Services and Applications : Opportunities and Best Practices for the Healthcare Industry," in *Enterprise Networking and Computing in Healthcare Industry*, 2003, no. September, pp. 159–160.
[5] U.S. Department of Health & Human Services, "Understanding Health Information Privacy." [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/. [Accessed: 21-May-2013].
[6] H. DeYoung, D. Garg, and L. Jia, "Experiences in the logical specification of the HIPAA and GLBA privacy laws," in *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, 2010, pp. 73–82.
[7] a. Barth, A. Datta, J. C. Mitchell, and H. Nissenbaum, "Privacy and contextual integrity: framework and applications," in *IEEE Symposium on Security and Privacy*, 2006, p. 15 pp.–198.
[8] P. E. Lam, J. C. Mitchell, and S. Sundaram, "A Formalization of HIPAA for a Medical Messaging System," in in *Trust, Privacy and Security in Digital Business*, 8th ed., vol. 5695, S. Fischer-Hübner, C. Lambrinoudakis, and G. Pernul, Eds. Springer Berlin Heidelberg, 2009, pp. 73–85.
[9] M. Backes, B. Pfitzmann, and M. Schunter, "A toolkit for managing enterprise privacy policies," *Computer Security–ESORICS 2003*, no. October, pp. 162–180, 2003.
[10] L. F. Cranor, *Web Privacy with P3P*. O'Reilly & Associates, 2002, pp. 1–344.